Terrorists Continue to Impersonate Military and Civilian Officials to Further Attacks

Impersonation or the use of uniforms and identification (name plates, badges, rank insignia, unit identification) of military, law enforcement, airport, delivery service, and emergency services personnel to gain access to attack sites, to transport weapons, to conduct preoperational planning, or to carry out a secondary attack is a feature used by many terrorists overseas. Uniforms are available by theft, counterfeit manufacture, and purchase on the Internet, such as auction sites.

The use of first responder uniforms provides terrorists the opportunity to conduct a secondary attack. Terrorists are able to gain access to a primary attack site and conduct a secondary attack by using emergency response vehicles or dressing as emergency response personnel.

The FBI has no creditable intelligence suggesting foreign or domestic terrorists are considering the use of deception tactics to conduct attacks against the Homeland. Nonetheless, these tactics are widely known and used elsewhere. The public's trust in first responders and the security community make terrorist deception involving the impersonation of these officials especially effective. Terrorist use of official first responder uniforms and identification would likely afford a higher level of access.

Suggested Protective Measures

Facility and program managers can take a variety of protective measures to detect possible terrorist deception tactics:

Immediately report the theft or loss of uniforms, badges, and other uniform components;

Companies responsible for manufacturing or laundering official uniforms should report any questionable activity surrounding the loss or procurement of uniforms;

All persons wearing company uniforms should have their employment and identities confirmed prior to admittance into potential target areas; and,

Security managers should employ other security measures to ensure uniforms are not the sole means of identification for authorized access.

Reporting Notice

Immediately report suspicious or criminal activity potentially related to terrorism to the local Federal Bureau of Investigation (FBI) Joint Terrorism Task Force and the Department of Homeland Security National Operations Center (NOC). The FBI regional phone number can be found at www.fbi.gov/contact/fo/fo.htm. The NOC can be reached via telephone at 202-282-8101 or by e-mail at HSCenter@dhs.gov.

Source: FBI Intelligence Bulletin, Directorate of Intelligence

Information is classified "Unclassified/For Official Use Only".

United States: Police and General Aviation Security

In the United States, there are approximately 650 airports certified for scheduled airline service. There are also approximately 19,983 landing facilities available to general aviation. The Aircraft Owners and Pilots Association has partnered with the Transportation Security Administration to develop a nationwide Airport Watch Program that uses the more than 674,500 pilots as eyes and ears for observing and reporting

suspicious activity. Airports range from just one person running the entire operation to a formal airport management team with several people managing the airport. Some general aviation airports have U.S. Customs personnel permanently assigned there and also have professional and dedicated crash and rescue personnel assigned as well.

A properly certified pilot must have the following documents in their possession: a pilot's license issued by the Federal Aviation Administration (FAA); a medical certificate which is issued by a designated Aviation Medical Examiner; and a government-issued photo identification card such as a passport or driver's license. By federal law, these documents must be given to a law enforcement officer upon request. In addition, the pilot must be able to produce the following documents for the aircraft they are operating: airworthiness certificate, registration, operating handbook, and weight and balance information.

All aircraft registered in the U.S. have a unique number, much like a license plate. This number is known as an N-number, because all U.S. registered aircraft start with the letter N, or tail number. The FAA maintains a public database that can be used in a preliminary investigation to check airman certificates and N-numbers. The database can be accessed through the FAA web site at faa.gov. Any information obtained at this site should be confirmed with the FAA and should never be used as the basis of official action.

Source: www.officer.com TSA

Information is classified "Restricted to Law Enforcement Only".

eBay/PayPal Complete Law Enforcement Guide

eBay, Inc., has established a Fraud Investigations Team (FIT) to promote safe use of their platforms and encourage prosecution of those responsible for misconduct on them. Law enforcement agencies in North America seeking assistance and records for investigations that relate to either eBay or PayPal should use the **Frequently Asked Questions** found as guidance in how FIT can assist in these investigations at: http://www.policelink.com/training/articles/list?article_search%58category-id%50=24-investigations, click on the search feature, enter eBay/PayPal Complete Law Enforcement Guide.

If your specific question is not answered at this site, please contact FIT directly for information by phone at 408-967-9919. All calls are returned within **ONE** business day.

Source: Information taken from Armstrong Atlantic State University, Law Enforcement Bulletin, Center for Justice Administration

Information is classified "Intended Only For Use by Law Enforcement".

IACP Publications Aimed at Enhancing Law Enforcement's Ability to Monitor Sex Offenders

In collaboration with the American Probation and Parole Association, the International Association of Chiefs of Police has released two new publications aimed at enhancing law enforcement's ability to monitor and track sex offenders in the community.

> *Strategically Monitoring Sex Offenders: Accessing Community Corrections' Resources to Enhance Law Enforcement Capabilities*, a publication that identifies tools and information used by correctional agencies can benefit law enforcement's ability to monitor and track sex offenders.
>
> *Tracking Sex Offenders with Electronic Monitoring Technology: Implications and Practical Uses for Law Enforcement*, a publication that defines and provides examples of electronic monitoring technology, discusses law enforcement involvement with electronic monitoring technology, outlines the benefits and concerns of using this technology, and highlights key considerations for the law enforcement community.

To access these resources and other sex offender management resources, please visit http://www.iacp.org/profassist/ReturningOffenders.htm.

To request copies of the above sex offender management related products or for more information on IACP sex offender management efforts, please contact: Sarah Wygant, Training Coordinator, at 800-THE-IACP, Ext. 830.

Security Awareness: Hotel Security Connections

Jet-setting federal workers and law enforcement are cautioned regarding the use of the Internet connections supplied by hotels, as most are not secured properly, according to a new study from the Cornell University of Hotel Administration. One hundred forty-seven hotels responded to a written survey sent out by the researchers, asking about each hotel's network infrastructure. The hotels surveyed ranged from family-oriented hotels to those serving more of a business clientele. The study found 20% of hotel networks use simple hub topologies, in which every packet from every user gets broadcast to every other user. This is an unsecured network researchers warned.

In addition to the wired networks, about 90% of hotels offered wireless access, which operates in a hub-like setup. The majority of other hotels managed patron traffic through switches or routers, which are slightly more secure than hubs, but they still have shortcomings. Switchers and routers direct Internet packets only to the appropriate recipients, rather than to all parties on the network. Users on such networks could still be vulnerable to man-in-the-middle attacks. In these scenarios, an attacker's computer broadcasts itself as the Internet gateway for the hotel and intercepts all traffic going to and from the Internet. In wireless environments attackers could set rogue hot spots which would mimic a similar spoof.

The researchers recommend for maximum security hotels should set up Virtual Local Area Networks (VLANs). If hotels were to set up VLANs on all ports in the hotel – that is to make every single room its own VLAN – the chances for Address Resolution Protocol spoofing and other hacks are minimized.

For those using hotel networks, the researchers recommended ensuring that your computer has an updated firewall, and that any sensitive transaction you undertake uses secure socket layer (SSL) protocol, as evidenced by the "https" prefix of the web address. Use a virtual private network or SSL-based e-mail when possible.

The survey reported 20.6 % of the hotels reported malicious activity had taken place on their networks.

Source: Transportation Security Administration (TSA), TSA's representative to FBIHQ National Joint Terrorism Task Force

United States Department of Justice, Office of Community Oriented Policing Services Holds Conference Calls Regarding Crime and Public Safety

On October 29, 2008 and October 30, 2008, the United States Department of Justice, Office of Community Oriented Policing Services (COPS) held the first of two in a series of conference calls regarding crime and public safety issues affected by the nation's current economy. Members of both the local and federal law enforcement community, as well as representatives from private industry and academia, joined these calls to discuss recent trends in mortgage fraud and metal theft, crimes which have increased due to the rising number of foreclosures hitting all areas of the country.

Detectives and investigators expressed the general belief the sheer number of mortgage fraud and related investigations will require more and more resources from local law enforcement agencies. Many police departments, however, have only one or two detectives dedicated to handling these cases, which require special training in financial investigations. Multiple participants emphasized the need for training and curriculum devoted specifically to mortgage fraud, equity skimming, and other similar scams.

Another growing crime issue is the rampant metal theft hitting urban, suburban, and rural areas alike. Some departments have reported copper theft has declined, perhaps owing to the decrease in the price of copper in recent months and new legislation passed by a number of states. However, thieves have simply adapted to these changes, as police have noticed an increase in the theft of catalytic converters and other metals.

Many police departments from across the country have responded to mortgage fraud and metal theft by forming partnerships with key stakeholders in the issue. Financial crimes investigators stressed the importance of working cooperatively with the FBI, as well as state and district attorney's offices, in addressing mortgage fraud and equity theft cases. Metal theft detectives, meanwhile, emphasized the need to work with and educate metal recyclers, in order to reduce thefts successfully.

The COPS Office will follow-up these conference calls by posting lists of resources for law enforcement officers on the COPS web site, as well as scheduling additional calls in the future. Further, a Problem-Oriented Policing Guide on metal theft is due out in 2009 and will be available through the COPS web site at http://cops.usdoj.gov. For more information about these issues, please contact the author at zoe.mentel@usdoj.gov.

Domestic Violence Instructor Training Program (DVITP)

This program is designed to increase the effectiveness of law enforcement professionals tasked with delivering domestic violence related training. The primary focus of this program is to develop adjunct Federal Law Enforcement Training Center (FLETC) instructors who will be required to redeliver this material in their respective jurisdictions. Participants will learn new and creative ways to present various domestic violence related topics such as Dynamics of Domestic Violence, Officer Safety, Law Enforcement Liability and Determining Predominant Aggressor.

Who Should Attend

Applicants must be federal, state, local, campus or tribal criminal justice professionals, law enforcement personnel, or domestic violence advocates. Participants must have prior training in responding to domestic violence crimes and have some experience training these issues. In addition, participants must represent agencies with needs or anticipated needs for domestic violence training.

Tuition and Cost

Tuition is free.

Training Dates

Arlington, Texas – January 26, 2009 to January 30, 2009
Lakeland, Florida – February 16, 2009 to February 20, 2009
Grand Island, Nebraska – March 23, 2009 to March 27, 2009
Edina, Minnesota – April 13, 2009 to April 17, 2009
Sioux Falls, South Dakota – June 15, 2009 to June 19, 2009

Contact Information

For additional information, please contact stateandlocaltraining@dhs.gov or call 800-74FLETC.

To submit law enforcement information for publication in OLEC's Heads Up, please contact: Valeria White, Management and Program Analyst (MPA), Office of Law Enforcement Coordination (OLEC), Director's Office (DO), Federal Bureau of Investigation (FBI), at 202-436-8208, intranet e-mail White, Valeria F., or internet e-mail Valeria.White@ic.fbi.gov.